3G AND 4G SMARTPHONE SECURITY

Understanding security and encryption on mobile networks

Executive Summary

The smartphone is the most commonly used communications device in the modern world. 72% of Americans, 59% of Turks, and 88% of Koreans use them. Virtually every business executive, politician, and military leader uses a 3G or 4G smartphone. Thus, it is ironic that key holders of corporate and national security secrets rely on a communication device that is virtually devoid of security.

Discrete communications are widely intercepted. One has only to read the news to recognize that "secret" national security discussions by the leaders of Turkey, Germany, USA, and many others have been recorded and publicly released. Clearly, purportedly secured communications are anything but. And the most unsecured communications involve 3G and 4G mobile devices.

3G and 4G Encryption

It is often repeated that 3G is encrypted and 4G is not. This is only true from a basic sense. In reality neither should be considered encrypted sufficiently for national security. First, both 3G and 4G refer to radio frequency (RF) protocols broadcast between the mobile and the Base Transceiver Station (BTS) on the tower. As a radio signal, the communications between the device and the BTS are easily intercepted and recorded.

3G employs an encryption protocol known as A5/1, which was demonstrated to be cracked by a single PC in two hours. Today, the methods and tools to decrypt A5/1 are commonly available on the internet, and devices which include the A5/1 decryption may also be purchased on the internet. Thus, the 3G A5/1 encryption is effectively useless against even elementary interception. Some networks employ newer encryption protocols, but that offers but a minor deterrence to serious hackers.

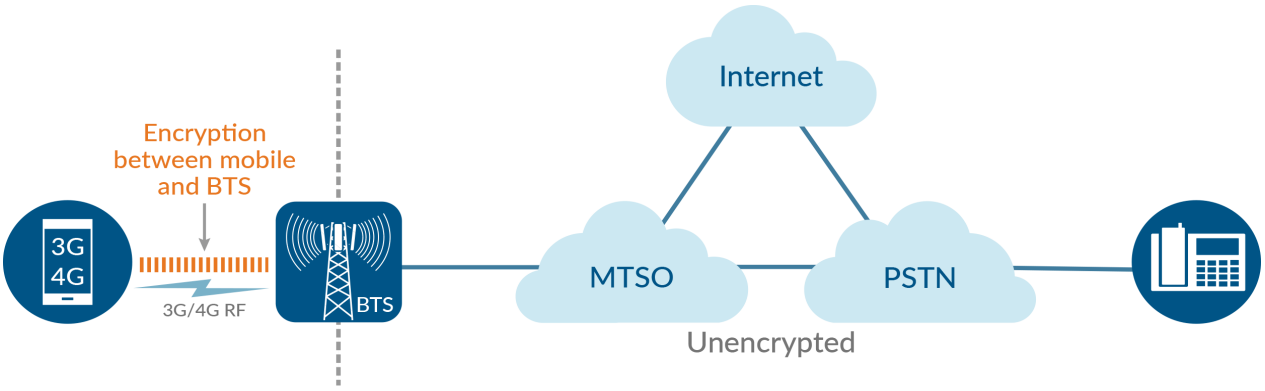

Figure 1. 3G/4G encryption is not end-to-end. Only the RF between the mobile device and the BTS might be encrypted.

REDCOM®

www.redcom.com

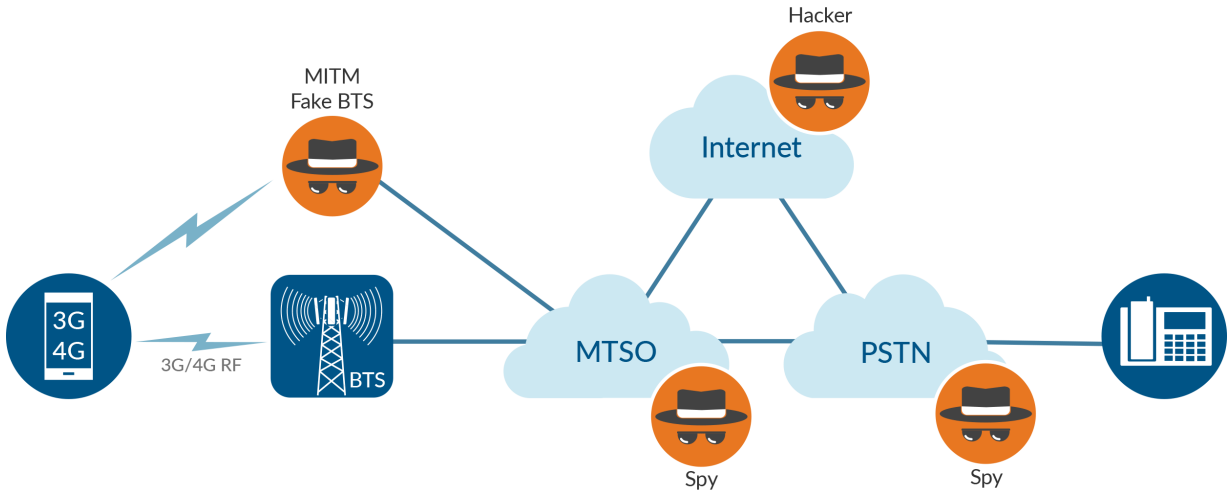

Figure 2. Security concerns exist everywhere on an unsecure network. A Man-in-the-Middle (MITM) with a false BTS unit can intercept mobile communications. Additionally, external hackers or even spies inside the network can listen in on conversations.

4G in itself has no inherent encryption of the RF signal. It does, though, offer improved authentication, as well as AES and two other encryption methods. But offer — as opposed to employ — does not guarantee any level of encryption since the level of encryption is dictated by the capabilities of the BTS and mobile operator. In short, neither 3G nor 4G offer any assurance that the RF communications between the mobile and the BTS are secure.

Man-in-the-Middle (MITM) Interception

Law enforcement agencies in the USA and other countries employ false BTS units that emulate those of mobile carriers. This is known as Man-in-the-Middle (MITM) interception and is quite commonly used to violate IP-based networks. These MITM devices pretend to be a mobile BTS, coordinate an encryption key with the mobile device, intercept the communications, and pass it back to the mobile carrier or the PSTN. The mobile user has no idea that the communications have been compromised. And, since the MITM BTS knows the encryption key, it can easily decrypt communications before forwarding it to a lawful network.

Like RF interception devices, these MITM fake BTS devices are available to governments and naturally are available on the black market. As a result, 3G and 4G communications- encrypted or otherwise- cannot be considered to be secure.

Encrypted vs. Secure

Encryption of digitally conveyed communications is a mechanism to scramble all or part of a message such that patterns are not readily identifiable and thus cannot be recompiled into the original form until decrypted by another device.

Security is a much broader consideration. Encryption is merely a part of a full security plan, which also involves network design and, more important, human behavior. As observed prior to the US elections, individuals used unencrypted devices even while encrypted devices were available.

Examination of Encryption

Modern digital communications (e.g., VoIP) encryption mechanisms scramble the message with the use of a standardized unique key which is known only to the devices on either end of a connection. Typically, the key used for the popular Advanced Encryption Standard (AES) is 128 bits in length.

Cinematic films have popularized the scene of the good guy entering codes (keys) in order to guess the correct key/password to decrypt the information. This is known as the Brute Force method. But while popular in movies, Brute Force would require a billion billion years (yes, that is a billion times a billion years) to decrypt one message. In fact, to this date AES 128 has never been broken with Brute Force.

That is not to say that AES 128 has not been deciphered. The most common "secure" VoIP encryption protocol is Secure Real Time Protocol (SRTP) which uses AES 128 encryption. However, oddly enough, if SRTP is sent over non-encrypted medium (as is commonly done) then the key is sent unencrypted. This is equivalent to locking one's home but leaving the key hanging on the front door. In order to benefit from the AES 128 encryption, SRTP must always be sent over Transport Layer Security (TLS).

3G and 4G Encryption is Meaningless to Security

Even if 3G and 4G were properly encrypted, it must be recognized that these terms refer only to the RF signal between the device and the BTS. To make it perfectly clear: 3G/4G encryption is not between the two devices. In almost all cases, the BTS decrypts the communications and passes it through the mobile network, the PSTN, and/or the government network totally unencrypted.

Besides MITM interception of 3G and 4G RF communications, great risk also resides once the unencrypted communications are inside the fixed network(s). It should be no surprise to anyone that IP-based networks have been regularly compromised. Networks based on Signaling System 7 (SS7 or C7) offer little added security, as these have been demonstrated to be hacked by external forces, and communications recorded. Those concerned about secure communications should consider no mobile, public, private, or government network to be secure.

While hacking by foreign agencies or domestic enemies is a grave concern, it pales in comparison to the real problem-internal interception and dissemination of communications. That is, a person with inside access to the network's decrypted communications with virtually no impediment to intercepting 3G, 4G, VoIP, and other technologies. Virtually all of Wikileak's tens of thousands of state secrets were internally intercepted; U.S. president Donald Trump's calls to Russia were internally intercepted. Turkey as well has made international news with voice conversations internally intercepted. It should be perfectly clear that the primary concern is not 3G/ 4G encryption, but total network security and encryption from end device to end device.

Security for Smartphones

With the networks that carry communications so easily compromised, it is obvious that the only way to secure 3G and 4G (as well as VoIP) communications is with appropriate encryption from device to device, with the encryption carried uninterrupted throughout all networks in which the communications may pass. Only in this manner may communications be secured against enemies external and internal, foreign and domestic.

Fortunately, a solution does exist. REDCOM's Sigma Client is an app that provides end-to-end total AES 128 encryption between smartphones, PCs, and VoIP phones/video terminals. With Sigma Client on both the originating

and terminating smart devices, and an IP transport network in between, all voice, chat, and video is encrypted to a standard that has never been broken.

As a client application, Sigma Client ensures complete encryption through 3G, 4G, public (IP-PSTN), and packet-based government networks. This alleviates the real risks of external as well as internal interception. REDCOM's Sigma® Core encryption server provides authentication (authorization of use) as well as access control (who is permitted to call who/where; e.g., prohibiting calls out of country).

As an added bonus, REDCOM's Sigma Core encryption server can provide end-to-end AES 128 encryption to not just 3G and 4G mobiles, but also to VoIP phones, IP video terminals, and even the Sigma Client app on Windows PCs.

Considering the damage caused by international espionage and the lack of security with 4G, can any agency continue with such incredible risk? It would be foolish to do so, given that a solution readily exists and is available today.

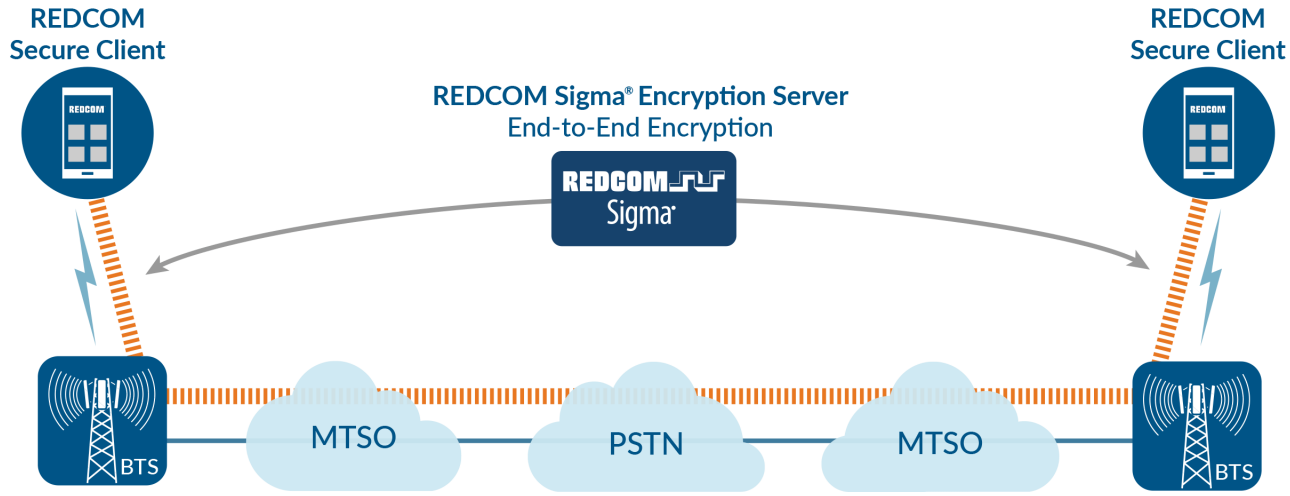

Figure 3. Achieve end-to-end encryption with REDCOM's Sigma Client, which encrypts all voice, video, and chat communications with AES 128 encryption that has never been broken.

©2019 REDCOM Laboratories, Inc. REDCOM and the REDCOM logo are registered trademarks of REDCOM Laboratories, Inc.
Subject to change without notice or obligation.